

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-032006

(43)Date of publication of application : 29.01.2004

(51)Int.Cl.

H04L 12/56

H04L 12/46

(21)Application number : 2002-180693

(71)Applicant : FUJITSU LTD

(22)Date of filing : 21.06.2002

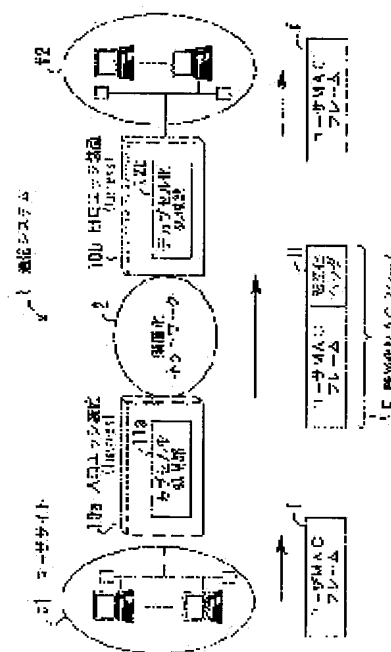
(72)Inventor : OKUDA MASAHIITO

(54) COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To improve a scalability and an operation efficiency by forming a VPN having constants set to be larger than constants in the prior art.

SOLUTION: A capsulizer 11a receives a user MAC frame (f) from a user site #1, and attaches a layer header H to set an arbitrary VPN thereto to capsulize the user MAC frame (f) and to generate a layer MAC frame F. A decapsulizer 12b receives the layer MAC frame F, and, when an edge destination address is the address of its own subscriber interface based on the layer header H and recognized to have been transmitted from an edge node device in an identical virtual LAN, extracts the user MAC frame f from the layer MAC frame F and decapsulizes it.



LEGAL STATUS

[Date of request for examination] 20.05.2005

[Date of sending the examiner's decision of rejection] 13.03.2007

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号
特開2004-32006
(P2004-32006A)

(43) 公開日 平成16年1月29日(2004.1.29)

(51) Int.Cl. ⁷	F I	テーマコード (参考)
H 0 4 L 12/56	H 0 4 L 12/56	5 K 0 3 0
H 0 4 L 12/46	H 0 4 L 12/46	5 K 0 3 3

審査請求 未請求 請求項の数 5 O L (全 20 頁)

(21) 出願番号	特願2002-180693 (P2002-180693)	(71) 出願人	000005223
(22) 出願日	平成14年6月21日 (2002. 6. 21)		富士通株式会社
			神奈川県川崎市中原区上小田中4丁目1番1号
		(74) 代理人	100092152
			弁理士 服部 毅巖
		(72) 発明者	奥田 将人
			神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
		Fターム(参考)	5K030 GA14 HC01 HC13 HD01 HD06 LB19 MD04 MD06 5K033 AA09 CB11 DA06 EC01 EC03

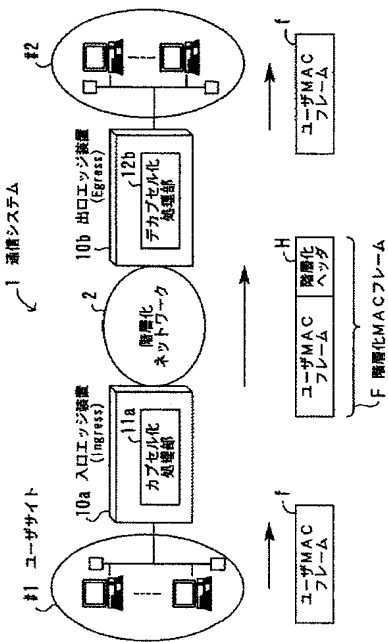
(54) 【発明の名称】 通信システム

(57) 【要約】

【課題】従来の設定数を超えてVPNを構成できるようにして、スケーラビリティ及び運用効率の向上を図る。

【解決手段】カプセル化処理部11aは、ユーザMACフレームfをユーザサイト#1から受信し、任意のVPNを設定するための階層化ヘッダHを付与して、ユーザMACフレームfをカプセル化し、階層化MACフレームFを生成する。デカプセル化処理部12bは、階層化MACフレームFを受信し、階層化ヘッダHにより、エッジ宛先アドレスが自己の加入者インタフェースのアドレスであり、かつ同一VLAN内の入口エッジ装置から送信されてきたことを認識した場合に、階層化MACフレームFからユーザMACフレームfを取り出してデカプセル化する。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

VPNの通信サービスを行う通信システムにおいて、ユーザMACフレームをユーザサイトから受信し、加入者インタフェースのアドレスであるエッジ送信元アドレス及び前記ユーザMACフレームを送信すべき出口エッジ側の加入者インタフェースのアドレスであるエッジ宛先アドレスを含み、任意のVPNを設定するための階層化ヘッダを付与して、前記ユーザMACフレームをカプセル化し、階層化MACフレームを生成するカプセル化処理部を有し、階層化ネットワークの入口エッジ側に配置される入口エッジ装置と、前記階層化MACフレームを受信し、前記階層化ヘッダにより、前記エッジ宛先アドレスが自己の加入者インタフェースのアドレスであり、かつ同一VLAN内の入口エッジ装置から送信されてきたことを認識した場合に、前記階層化MACフレームから前記ユーザMACフレームを取り出してデカプセル化するデカプセル化処理部を有し、前記階層化ネットワークの出口エッジ側に配置される出口エッジ装置と、を有することを特徴とする通信システム。

【請求項 2】

前記カプセル化処理部は、ユーザMACフレームからユーザヘッダを抽出してユーザ宛先アドレスを取得するユーザヘッダ抽出部と、ユーザ宛先アドレスとエッジ宛先アドレスとの対応テーブルであるカプセル化テーブルにもとづき、取得されたユーザ宛先アドレスをキーにして、エッジ宛先アドレスの検索を行うテーブル検索部と、検索成功時は、検索されたエッジ宛先アドレスと、エッジ送信元アドレスとを含む階層化ヘッダを生成する階層化ヘッダ生成部と、前記ユーザMACフレームに前記階層化ヘッダを付与する階層化ヘッダ付与部と、階層化MACフレーム用のFCSを計算するFCS計算部と、から構成されることを特徴とする請求項 1 記載の通信システム。

【請求項 3】

テーブル検索失敗時、前記階層化ヘッダ生成部は、宛先アドレスリストの各アドレスと、エッジ送信元アドレスとを含む複数の階層化ヘッダの生成、またはマルチキャストアドレスと、エッジ送信元アドレスとを含む複数の階層化ヘッダの生成のいずれかの生成処理を行い、前記階層化ヘッダ付与部は、ユーザMACフレームをコピーして、複数の階層化ヘッダをそれぞれ付与することを特徴とする請求項 2 記載の通信システム。

【請求項 4】

前記デカプセル化処理部は、階層化ヘッダにより、エッジ宛先アドレスが自己の加入者インタフェースのアドレスであるか、かつ同一VLAN内の入口エッジ装置から送信されてきたフレームであるかを判断して有効性のチェックを行う有効性チェック部と、前記階層化ヘッダのエッジ送信元アドレスとユーザヘッダのユーザ送信元アドレスとの対応をカプセル化テーブルに学習するアドレス学習部と、階層化MACフレームから前記階層化ヘッダを分離してユーザMACフレームを生成する階層化ヘッダ分離部と、ユーザMACフレーム用のFCSを計算するFCS計算部と、から構成されることを特徴とする請求項 1 記載の通信システム。

【請求項 5】

前記入口エッジ装置は、それぞれ異なるVLANのユーザサイトから、VLANタグ付きのユーザMACフレームを、1つのポートで複数受信する場合、VLAN毎に割り当てたポートのアドレスと、VLAN毎に割り当てたカプセル化テーブルと、を設けてVLANに対応した階層化ヘッダを生成することを特徴とする請求項 1 記載の通信システム。

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

本発明は通信システムに関し、特にVPN (Virtual Private Network: 仮想私設網) の通信サービスを提供する通信システムに関する。

【0002】

【従来の技術】

マルチメディアの進展に伴い、LAN (Local Area Network) 等の情報ネットワークに対する要求が多様化してきている。LANの規格としては、イーサネット (Ethernet:登録商標) が最も広く用いられており、従来、イーサネットは、同一敷地内の比較的狭い範囲でのネットワーク通信に使用されていた。

【0003】

一方、近年になってインターネットなどのデータトラフィックの急増に伴い、ネットワークのブロードバンド化が進行しており、同時に低コストのネットワーク・サービスが要求されている。

【0004】

このため、イーサネットは、LANだけでなく、公衆回線も包含したMAN (Metropolitan Area Network) やWAN (Wide Area Network) などにおいても広く利用されてきている。

【0005】

また、ネットワーク・サービスとして、通信事業者は、主に企業ユーザに対して、VPN サービスを提供することが実現化されている。VPNとは、社内で構築したネットワークを使って、通信事業者のサービスを、あたかも専用線のように利用できるサービスの総称である。

【0006】

一般にVPNは、レイヤ3 (ネットワーク層) をベースにしたVPN (L3VPN) と、レイヤ2 (データリンク層) をベースにしたVPN (L2VPN) とに大別されるが、現状では、レイヤ3プロトコルを限定することなく拠点間を接続して、柔軟な仮想ネットワークを構築することができるL2VPNへの需要が高まっている。

【0007】

このL2VPNのサービスを実現するために、イーサネットのブリッジネットワーク (レイヤ2でフレームを中継するネットワーク) では、IEEE802.1Qに既定されるVLAN (Virtual Local Area Network) タグを利用する。

【0008】

VLANとは、物理的なLAN構成とは独立に、ネットワークに接続した端末を仮想的 (論理的) にグループ化したLANのことで、1つのVLANが1つのブロードキャストドメインになる。また、イーサネットフレーム中にVLANタグ (4オクテット) が挿入されることにより、VLAN機能を実装したスイッチによって、VLANの決定処理等が行われる。

【0009】

図18はVLAN使用時のフレームフォーマットを示す図である。イーサネットver2のフレーム (TCP/IPで最もよく使われるイーサネットフレームである) にVLAN-Tagが挿入されたフォーマットを示している。

【0010】

DA (Destination Address) は、6オクテットの宛先MAC (Media Access Control) アドレスであり、SA (Source Address) は6オクテットの送信元MACアドレスである。

【0011】

タイプは、2オクテットでレイヤ3のプロトコルの識別番号が入る (例えば、レイヤ3がIPならば0x0800となる)。ペイロードは、イーサネットが運ぶデータであり、最大が1500オクテットである。FCS (Frame Check Sequence) は、エラーチェックを行うためのフィールドであり、エラーチェック対象は、DAからペイロードまでである。

【0012】

一方、4オクテットのVLANタグは、2オクテットのTPID (Tag Protocol ID) と2オクテットのTCI (Tag Control Information) 50

n) から構成され、イーサネットフレームの SA フィールドとタイプフィールドの間に挿入される。

【0013】

TPID は、VLAN-ID (VID) が挿入されていることを示すフィールドであり (タグ付きフレームであることを示すフィールドであり)、この場合 0x8100 である。

【0014】

TCI はタグ情報を格納する。タグ情報として、プライオリティは、IEEE802.1p で規定される 3 ビットの優先度情報、CFI (Canonical Format Identifier) は、1 ビットのインジケータ (イーサネットの場合は “0” を設定)、VID は、12 ビットの VLAN 識別子である。

10

【0015】

【発明が解決しようとする課題】

しかし、上記で説明したように、IEEE802.1Q 規定の VLAN タグは、12 ビットの VLAN-ID しか持たないため、VPN が 4094 個 ($2^{12} = 4096$ であるが、実際は、all “0”、all “1” は特殊用途に予約されているため 4094 個) しか実現できない。

【0016】

このため、従来の VLAN-ID では、通信事業者が 4094 を超えて、企業に対して VPN サービスを提供することができず、スケーラビリティ (拡張性) が低いといった問題があった。

20

【0017】

本発明はこのような点に鑑みてなされたものであり、イーサネットを利用したブリッジネットワーク上に、従来の設定数を超えて VPN を構成できるようにして、スケーラビリティ及び運用効率の向上を図った通信システムを提供することを目的とする。

【0018】

【課題を解決するための手段】

本発明では上記課題を解決するために、図 1 に示すような、VPN の通信サービスを行う通信システム 1 において、ユーザ MAC フレーム f をユーザサイト #1 から受信し、加入者インタフェースのアドレスであるエッジ送信元アドレス及びユーザ MAC フレーム f を送信すべき出口エッジ側の加入者インタフェースのアドレスであるエッジ宛先アドレスを含み、任意の VPN を設定するための階層化ヘッダ H を付与して、ユーザ MAC フレーム f をカプセル化し、階層化 MAC フレーム F を生成するカプセル化処理部 11a を有し、階層化ネットワーク 2 の入口エッジ側に配置される入口エッジ装置 10a と、階層化 MAC フレーム F を受信し、階層化ヘッダ H により、エッジ宛先アドレスが自己の加入者インタフェースのアドレスであり、かつ同一 VLAN 内の入口エッジ装置から送信されてきたことを認識した場合に、階層化 MAC フレーム F からユーザ MAC フレーム f を取り出してデカプセル化するデカプセル化処理部 12b を有し、階層化ネットワーク 2 の出口エッジ側に配置される出口エッジ装置 10b と、を有することを特徴とする通信システム 1 が提供される。

30

【0019】

ここで、カプセル化処理部 11a は、ユーザ MAC フレーム f をユーザサイト #1 から受信し、加入者インタフェースのアドレスであるエッジ送信元アドレス及びユーザ MAC フレーム f を送信すべき出口エッジ側の加入者インタフェースのアドレスであるエッジ宛先アドレスを含み、任意の VPN を設定するための階層化ヘッダ H を付与して、ユーザ MAC フレーム f をカプセル化し、階層化 MAC フレーム F を生成する。デカプセル化処理部 12b は、階層化 MAC フレーム F を受信し、階層化ヘッダ H により、エッジ宛先アドレスが自己の加入者インタフェースのアドレスであり、かつ同一 VLAN 内の入口エッジ装置から送信されてきたことを認識した場合に、階層化 MAC フレーム F からユーザ MAC フレーム f を取り出してデカプセル化する。

40

【0020】

50

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照して説明する。図1は本発明の通信システムの原理図である。通信システム1は、入口エッジ装置(Ingress)10aと、出口エッジ装置(Egress)10bとから構成され、階層化ネットワーク2を介して、VPNの通信サービスを提供するシステムである。ここで、2つ(2階層)のヘッダ情報(ユーザMACフレームf内のユーザヘッダと、後述の階層化ヘッダH)を持つフレームが流れるネットワークのことを本発明では階層化ネットワークと呼ぶ。

【0021】

また、入口エッジ装置10aにはユーザサイト(LANである) #1が接続し、出口エッジ装置10bにはユーザサイト #2が接続している。なお、入口エッジ装置10aと出口エッジ装置10bの本発明の機能は、実際には1台の同一の通信装置内に含まれるものである。 10

【0022】

入口エッジ装置10aはカプセル化处理部11aを有する。カプセル化处理部11aは、ユーザMACフレームfをユーザサイト #1から受信すると、階層化ヘッダHを付与して、ユーザMACフレームfをカプセル化し、階層化MACフレームFを生成する。

【0023】

階層化ヘッダHは、任意のVPNを設定するためのヘッダであり、従来のVLANタグ内のVLAN-IDで決められるVPN数よりも、VPN数を拡張化できるヘッダである(すなわち、4094個のVPN以上のVPNを設定可能)。 20

【0024】

階層化ヘッダHには、加入者インタフェースのアドレス(例えば、ユーザMACフレームfが入力した、入口エッジ装置10aの物理ポートのアドレス)であるエッジ送信元アドレスと、ユーザMACフレームfを送信すべき出口エッジ側の加入者インタフェースのアドレス(例えば、階層化MACフレームFが出力される、出口エッジ装置10bの物理ポートのアドレス)であるエッジ宛先アドレスとが含まれる。

【0025】

出口エッジ装置10bはデカプセル化处理部12bを有する。デカプセル化处理部12bは、階層化MACフレームFを受信すると、階層化ヘッダH内のエッジ宛先アドレスが自己の加入者インタフェースのアドレスであり、かつ同一VLAN内の入口エッジ装置から送信されてきたことを認識した場合に、階層化MACフレームFからユーザMACフレームfを取り出してデカプセル化する。 30

【0026】

次に本発明の通信システム1をイーサネットの通信に適用した場合について以降詳しく説明する。図2はイーサネット通信における本発明のカプセル化イメージを示す図である。システム構成は図1と同様である。

【0027】

ここで、図1で上述した入口エッジ装置10aと出口エッジ装置10bは、レイヤ2のスイッチングを行うので、以降ではL2SW10a、L2SW10bと呼ぶ。さらに、階層化ネットワーク2は階層化イーサネット網2、ユーザMACフレームfはイーサネットフレームf、階層化MACフレームFは階層化イーサネットフレームF、階層化ヘッダHをEoE(Ethernet over Ethernet)ヘッダHと呼ぶ。 40

【0028】

ユーザサイト #1の端末3aからユーザサイト #2の端末3bへ向かうイーサネットフレームfは、SA(送信元MACアドレス)が端末3aのMACアドレスx0、DA(宛先MACアドレス)が端末3bのMACアドレスy0の情報を含むユーザヘッダを持ち、端末3aからL2SW10aへ送信される。

【0029】

L2SW10aは、イーサネットフレームfを受信すると、カプセル化处理部11aでは、EoEヘッダHを生成して、イーサネットフレームfに付与し、階層化イーサネットフ 50

フレームFを生成して階層化イーサネット網2へ流す。

【0030】

EoEヘッダHは、L2SW10aの加入者インタフェースに割り当てられたエッジ送信元アドレスX1であるSAと、ユーザサイト#2に接続するL2SW10bの加入者インタフェースに割り当てられたエッジ宛先アドレスY1であるDAと、カプセル化されていることを示すコードが記されたタイプ情報(Type)とからなる。そして、L2SW10aは、階層化イーサネットフレームFに対し、階層化イーサネット網2上で、EoEヘッダHのDAによるフォワーディングを行う。

【0031】

L2SW10bは、階層化イーサネットフレームFを受信する。すると、デカプセル化処理部12bでは、EoEヘッダHのDAが、到着したL2SW10bの加入者インタフェースのアドレスであり、かつ階層化イーサネットフレームFが同一VLAN内のL2SW10aから送信されてきたことを認識した場合に有効と判断し、階層化イーサネットフレームFからイーサネットフレームfを取り出してデカプセル化する。

【0032】

ここで、L2SW10aで、ユーザサイト#1からのイーサネットフレームf(VLANタグ付きのフレーム、VLANタグなしのフレームいずれでもよい)に対し、DAをアドレスY1としてEoEヘッダHでカプセル化することは、L2SW10aからL2SW10bへのパスにフレームを通すことと等しく、他のトラフィックから分離されていることになる。すなわち、VPNを構築しているといえる。

【0033】

階層化イーサネット網2は、複数のL2SWから構成されており、階層化イーサネットフレームFに対して、L2SW10aは、通常の学習処理とフォワーディング処理とを行うだけでよく、SA(アドレスX1)とDA(アドレスY1)間にパスが存在することを意識する必要はない。

【0034】

また、L2SW間を接続するパスは、EoEヘッダH内のDAとSAの組み合わせで定義されることになる。これにより、DA、SAのビット幅に応じて、任意のL2SW間で任意のVPNを設定することができる。

【0035】

本発明では、DA、SA共に48ビットとする。したがって、 2^{48} のL2SW間で任意のパス(すなわち、VPN)を設定することができる。このため、従来のVLAN-IDで設定できるVPN数を超えて、VPNを設定することが可能になる。

【0036】

次にL2SWの全体構成について説明する。図3はL2SWの構成を示す図である。なお、以降ではL2SW10a、10bを合わせてL2SW10と呼ぶ。L2SW10は、加入者インタフェース部101-1~101-n(総称して加入者インタフェース部101)、スイッチ部102、局側インタフェース部103-1~103-n(総称して局側インタフェース部103)から構成される。

【0037】

L2SW10の実装形態としては、1つのラックに、複数の加入者インタフェースカード(加入者インタフェース部101-1~101-n)と、1つのスイッチカード(スイッチ部102)と、複数の局側インタフェースカード(局側インタフェース部103-1~103-n)が搭載された構成をとる。なお、スイッチ部102は、加入者インタフェース部101と局側インタフェース部103との対応を、ラック内で物理的に接続するためのものである。

【0038】

加入者インタフェース部101は、加入者側I/O処理部13、カプセル化処理部11、デカプセル化処理部12、カプセル化テーブルT1、宛先アドレスリストT2、加入者側MAC部14から構成される。局側インタフェース部103は、局側MAC部15、局側

I/O処理部16から構成される。

【0039】

動作概要について説明する。まず、ユーザサイトから階層化イーサネット網2へ（カプセル化方向）のフレーム送信について説明する。加入者側I/O処理部13は、ユーザサイトからのイーサネットフレームfの入力処理を行う。カプセル化処理部11は、カプセル化テーブルT1または宛先アドレスリストT2にもとづいて、イーサネットフレームfをカプセル化して階層化イーサネットフレームFを生成する。加入者側MAC部14は、階層化イーサネットフレームFにスイッチタグを付けてスイッチ部102へ送信する。

【0040】

スイッチ部102は、受信した階層化イーサネットフレームFを、スイッチタグにもとづき、対応する局側インタフェース部103へスイッチングする。局側MAC部15は、階層化イーサネットフレームFからスイッチタグを取り外す。局側I/O処理部16は、EoEヘッダHのDAに対応するポートから、階層化イーサネットフレームFを出力する。

【0041】

次に階層化イーサネット網2からユーザサイトへ（デカプセル化方向）のフレーム送信について説明する。局側I/O処理部16は、階層化イーサネットフレームFの入力処理を行う。局側MAC部15は、階層化イーサネットフレームFにスイッチタグを付けてスイッチ部102へ送信する。スイッチ部102は、受信した階層化イーサネットフレームFを、スイッチタグにもとづき、対応する加入者インタフェース部101へスイッチングする。

【0042】

加入者側MAC部14は、階層化イーサネットフレームFからスイッチタグを取り外す。デカプセル化処理部12は、階層化イーサネットフレームFを受信すると、宛先アドレスリストT2にもとづき有効性のチェックを行い、またカプセル化テーブルT1にアドレス学習させて、その後に、階層化イーサネットフレームFからイーサネットフレームfを取り出してデカプセル化する。加入者側I/O処理部13は、イーサネットフレームf内のヘッダのDAに対応するポートから、イーサネットフレームFを出力する。

【0043】

ここで、カプセル化テーブルT1は、イーサネットフレームfのユーザヘッダのDA（ユーザ宛先アドレス）と、階層化イーサネットフレームFのEoEヘッダHのDA（エッジ宛先アドレス）との対応テーブルである。

【0044】

また、加入者インタフェース部101は、カプセル化テーブルT1のエントリにはエイジング処理を施し、DAからのフレームが一定時間存在しない場合には、そのエントリをカプセル化テーブルT1から削除する。また、宛先アドレスリストT2は、同一VLAN内のL2SWのDAがリスト化されているものである。

【0045】

次にカプセル化処理部11について図4、図5を用いて説明する。図4はカプセル化処理部の構成を示す図である。図5はカプセル化処理後の階層化イーサネットフレームを示す図である。

【0046】

カプセル化処理部11a（L2SW10a側のカプセル化処理部）に対し、ユーザヘッダ抽出部11a-1は、端末3aからのイーサネットフレームfより、ユーザヘッダを抽出し、DA（y0）をテーブル検索部11a-2へ通知する。

【0047】

テーブル検索部11a-2は、アドレスy0をキーにしてカプセル化テーブルT1aを検索する。図のカプセル化テーブルT1aでは、ユーザヘッダのDA（y0）とEoEヘッダのDA（Y1）が対応している（対応関係が登録されている場合、検索成功である）。

【0048】

検索成功時、テーブル検索部11a-2は、カプセル化テーブルT1aから取得したアド

10

20

30

40

50

レス (Y1) を E o E ヘッダ生成部 11a-3 へ通知する。E o E ヘッダ生成部 11a-3 は、アドレス (Y1) を DA、自アドレスレジスタの値 (ここでは X1) を SA にして、E o E ヘッダ H1 を生成する。

【0049】

E o E ヘッダ付与部 11a-4 は、イーサネットフレーム f に E o E ヘッダ H1 を付与する。FCS 計算部 11a-5 は、階層化イーサネットフレーム用に FCS を再計算する。そして、生成された階層化イーサネットフレーム F1 は、加入者側 MAC 部 14 へ転送される。

【0050】

一方、テーブル検索部 11a-2 が DA (y0) を検索した際に、カプセル化テーブル T1a に、アドレス情報が存在しない場合には検索失敗となる。このような場合、テーブル検索部 11a-2 は、検索が失敗した旨を E o E ヘッダ生成部 11a-3 へ通知する。

【0051】

E o E ヘッダ生成部 11a-3 は、検索失敗通知を受け取ると、宛先アドレスリスト T2a に記載されているアドレスを各 DA として E o E ヘッダを生成する。図 4、図 5 の場合では、アドレス Y1 を DA とした E o E ヘッダ H1 と、アドレス Z1 を DA とした E o E ヘッダ H1a との 2 つの E o E ヘッダを生成することになる。

【0052】

そして、E o E ヘッダ挿入部 11a-4 は、生成された E o E ヘッダの数分イーサネットフレーム f をコピーして (ここでは 2 つのイーサネットフレーム f を生成)、これらに E o E ヘッダ H1、E o E ヘッダ H1a を付与して FCS 計算部 11a-5 へ転送し、階層化イーサネットフレーム F1、F1a が生成されることになる。

【0053】

次にデカプセル化処理部 12 について説明する。図 6 はデカプセル化処理部の構成を示す図である。デカプセル化処理部 12b (L2SW10b 側のデカプセル化処理部) に対し、有効性チェック部 12b-1 は、階層化イーサネットフレーム F1 の E o E ヘッダ H1 の DA が自アドレスレジスタと等しいかチェックし、かつ、E o E ヘッダ H1 の SA が宛先アドレスリスト T2b に含まれているか否かをチェックする。

【0054】

ここでは、E o E ヘッダ H1 の DA と自アドレスレジスタは、ともに Y1 で等しく、かつ E o E ヘッダ H1 の SA (X1) は、宛先アドレスリスト T2b に含まれているため (E o E ヘッダ H1 の SA (X1) が宛先アドレスリスト T2b に含まれているということは、L2SW10b 側からフレームを返信する場合に、X1 は DA となるということ)、受信した階層化イーサネットフレーム F1 は、有効であると判断される (有効でなかった場合は廃棄する)。

【0055】

アドレス学習部 12b-2 は、E o E ヘッダ H1 の SA (X1) と、イーサネットフレーム f のユーザヘッダの SA (x0) との対応関係を学習し、その対応関係をカプセル化テーブル T1b に登録する (E o E ヘッダ H1 の SA (X1) と、ユーザヘッダの SA (x0) を登録しておくことにより、L2SW10b がカプセル化処理する場合に、DA としてこれらのアドレスが用いられる)。

【0056】

E o E ヘッダ分離部 12b-3 は、階層化イーサネットフレーム F1 より、E o E ヘッダ H1 を分離して、イーサネットフレームを FCS 計算部 12b-4 へ送信する。FCS 計算部 12b-4 は、イーサネットフレーム用に FCS を再計算する。そして、生成されたイーサネットフレーム f は、端末 3b 側へ転送される。

【0057】

次に階層化イーサネットフレーム F をマルチキャストする場合について説明する。図 7 は階層化イーサネットフレームのマルチキャストを示す図であり、図 8 はイーサネットフレームとマルチキャスト時の階層化イーサネットフレームを示す図である。

【0058】

階層化イーサネット網2内のL2SW10a、10b、10cは、同一VLANを構成している。また、L2SW10aと端末3aが接続し、L2SW10bと端末3bが接続し、L2SW10cと端末3cが接続している。さらに、端末3a～端末3cのMACアドレスはそれぞれx0、y0、z0とする。

【0059】

ここで、L2SW10aからL2SW10bへフレーム送信する場合について考える。L2SW10aは、ユーザヘッダとして、DAがy0でSAがx0のイーサネットフレームf0を端末3aから受信すると、カプセル化処理部11aは、アドレスy0をキーにしてカプセル化テーブルT1aを検索する。このとき、図に示すように、カプセル化テーブルT1aにアドレス情報が登録されていないとする。

【0060】

このような場合には、カプセル化処理部11aは、マルチキャストアドレスMC（あらかじめ設定されている）をDAとしたEoEヘッダHmcをイーサネットフレームf0に付与して、マルチキャスト用の階層化イーサネットフレームFmcを生成する。

【0061】

そして、同一VLAN内のL2SW（ここではL2SW10b、10c）へ階層化イーサネットフレームFmcをマルチキャストする。このようにして、階層化イーサネット網2内では、IEEE802.1に準拠して、マルチキャストアドレスMCを持った階層化イーサネットフレームFmcが転送される。

【0062】

以上説明したように、上述した図4、図5では、カプセル化処理において、カプセル化テーブルT1の検索失敗時、宛先アドレスリストT2に登録されているDAでEoEヘッダHを生成して階層化イーサネットフレームFを転送する構成としたが、図7、図8では、検索失敗時において、マルチキャストMCをDAとしたEoEヘッダHmcを生成して、階層化イーサネットフレームFmcを転送するものである。

【0063】

なお、マルチキャストされた階層化イーサネットフレームFmcをデカプセル化処理する場合は、デカプセル化処理部12の有効性チェック部では、判断項目が1つ増えて、EoEヘッダHのDAが自アドレスレジスタと等しいか、または設定されているマルチキャストアドレスと等しいかを判断することになる。その他の処理は図6と同様である。

【0064】

次に同一VLAN上において、階層化イーサネットフレームFが受信される様子について説明する。図9は階層化イーサネットフレームの受信イメージを示す図であり、図10は転送されるイーサネットフレーム及び階層化イーサネットフレームを示す図である。なお、カプセル化テーブルT1aでの検索が失敗して、宛先アドレスリストT2aにもとづいて、複数の階層化イーサネットフレームF2a、2bを転送する場合（マルチキャストでない場合）について示す。

【0065】

階層化イーサネット網2内のL2SW10a、10b、10cは、同一VLANを構成しており、L2SW10aと端末3aが接続し、L2SW10bと端末3bが接続し、L2SW10cと端末3cが接続している。また、端末3a～端末3cのMACアドレスはそれぞれx0、y0、z0である。

【0066】

ここで、L2SW10aからL2SW10bへフレーム送信する場合を考える。L2SW10aは、ユーザヘッダとして、DAがy0、SAがx0のイーサネットフレームf0を端末3aから受信すると、カプセル化処理部11aは、アドレスy0をキーにしてカプセル化テーブルT1aを検索する。このとき、図に示すように、アドレス情報がカプセル化テーブルT1aに登録されていないとする。

【0067】

このとき、カプセル化処理部11aは、宛先アドレスリストT2aにもとづいて、アドレスY1をDAとしたEoEヘッダH2aと、アドレスZ1をDAとしたEoEヘッダH2bとの2つのEoEヘッダを生成して、2つの階層化イーサネットフレームF2a、F2bを生成する。そして、L2SW10aは、階層化イーサネットフレームF2aをL2SW10bへ送信し、階層化イーサネットフレームF2bをL2SW10cへ送信する。

【0068】

L2SW10bに対し、デカプセル化処理部12bは、階層化イーサネットフレームF2aを受信し、ユーザヘッダのSA(x0)とEoEヘッダH2aのSA(X1)との関係を学習して、カプセル化テーブルT1bへ登録する。そして、L2SW10bは階層化イーサネットフレームF2aのデカプセル化処理を行って、イーサネットフレームf0を取り出して端末3bへ送信する。イーサネットフレームf0は、端末3bで受信されて処理される。

【0069】

L2SW10cに対し、デカプセル化処理部12cは、階層化イーサネットフレームF2bを受信し、ユーザヘッダのSA(x0)とEoEヘッダH2bのSA(X1)との関係を学習して、カプセル化テーブルT1cへ登録する。そして、L2SW10cは階層化イーサネットフレームF2bのデカプセル化処理を行って、イーサネットフレームf0を取り出して端末3cへ送信する。ただし、端末3cでは、イーサネットフレームf0が自分宛ではないので、このフレームは廃棄される。

【0070】

次に図9で上述したシステムに対して、L2SW10bからL2SW10aへフレーム応答を返信する場合について説明する。図11はフレーム応答を返信する様子を示す図であり、図12は転送されるイーサネットフレーム及び階層化イーサネットフレームを示す図である。

【0071】

L2SW10bからL2SW10aへフレーム送信する場合、L2SW10bは、ユーザヘッダとして、DAがx0、SAがy0のイーサネットフレームf1を端末3bから受信すると、カプセル化処理部11bは、アドレスx0をキーにしてカプセル化テーブルT1bを検索する。そして、カプセル化処理部11bは、DAがX1、SAがY1のEoEヘッダH3を付与して階層化イーサネットフレームF3を生成し、L2SW10aへ送信する。

【0072】

L2SW10aに対し、デカプセル化処理部12aは、階層化イーサネットフレームF3を受信して、有効性を確認すると、ユーザヘッダのSA(y0)とEoEヘッダH3のSA(Y1)との関係を学習して、カプセル化テーブルT1aへ登録する。

【0073】

そして、階層化イーサネットフレームF3のデカプセル化処理を行って、イーサネットフレームf1を取り出して端末3aへ送信する。イーサネットフレームf1は、端末3aで受信されて処理される。

【0074】

次にL2SW10の1つのポートに対し、それぞれ異なるVLANからのイーサネットフレームfが入出力する場合について説明する。図13はL2SW10aの1つのポートへ複数のイーサネットフレームが入力する場合の構成を示す図である。

【0075】

イーサネットスイッチ4には、ユーザサイト#1、#2が接続する。ユーザサイト#1には端末31~33が含まれ、ユーザサイト#2には端末#34~36が含まれる。端末31~36のMACアドレスをそれぞれx1~x6とする。また、ユーザサイト#1は、VLAN#1(VPN#1)に属し、ユーザサイト#2は、VLAN#2(VPN#2)に属する。

【0076】

10

20

30

40

50

イーサネットスイッチ4は、ユーザサイト#1から送信されたフレームにVLAN-ID#1を付与して、イーサネットフレームf_t-#1を生成し、またユーザサイト#2から送信されたフレームにVLAN-ID#2を付与してイーサネットフレームf_t-#2を生成する。そして、イーサネットスイッチ4から、VLAN#1のイーサネットフレームf_t-#1及びVLAN#2のイーサネットフレームf_t-#2が、L2SW10aに向けて送信される。

【0077】

このようにそれぞれ異なる複数のVLANからイーサネットフレームを受信する場合、L2SW10aでは、VLAN毎にカプセル化テーブルを保持する。ここでは、VLAN#1用カプセル化テーブルT1-1及びVLAN#2用カプセル化テーブルT1-2を保持 10
することになる。

【0078】

L2SW10aでは、入力したフレームがVLAN#1のイーサネットフレームf_t-#1ならば、VLAN#1用カプセル化テーブルT1-1で検索してカプセル化処理する。また、入力したフレームがVLAN#2のイーサネットフレームf_t-#2ならば、VLAN#2用カプセル化テーブルT1-2で検索してカプセル化処理する。このように、それぞれ異なるVLANに対応したカプセル化テーブルを用いることで、該当するVLANのEoEヘッダHのDAを効率よく設定することができる。

【0079】

また、L2SW10aのポートには、それぞれのVLAN用にアドレスを割り振っておく 20
。すなわち図の場合では、1つのポートのアドレスとして、VLAN#1ならばアドレスX1、VLAN#2ならばアドレスX2とする。このように、1つのポートに対して、VLANに対応したアドレスを設定しておくことで、該当するVLANのEoEヘッダHのSAを効率よく設定することができる。

【0080】

図14はL2SW10aの1つのポートへ複数のイーサネットフレームが入力する場合の構成を示す図である。図13ではイーサネットスイッチ4がVLAN-IDを付与したが、図14ではイーサネットスイッチ4でVLAN-IDの付与が行われない場合である。

【0081】

このような場合、L2SW10aでは、VLAN毎のカプセル化テーブルT1-1、T1 30
-2の他に、MACアドレステーブルT3を保持することになる。MACアドレステーブルT3は、端末のMACアドレスと、VLANとの対応テーブルである。

【0082】

ここでは、ユーザサイト#1内の端末31～33の送信元MACアドレスx1～x3とVLAN#1とが対応し、ユーザサイト#2内の端末34～36の送信元MACアドレスx4～x6とVLAN#2とが対応したテーブル構成となっている。

【0083】

VLAN-IDが付与されていないイーサネットフレームf_#1、f_#2が入力すると、L2SW10aでは、入力イーサネットフレームのSAからMACアドレステーブルT3 40
を検索して、対応するVLANを求め、そのVLANに該当するカプセル化テーブルを検索することになる。

【0084】

例えば、イーサネットフレームf_#1が端末31（MACアドレスx1）からのものとする 50
と、L2SW10aは、MACアドレステーブルT3からVLAN#1と認識する。そして、VLAN#1用のカプセル化テーブルT1-1を検索して、カプセル化処理を行う。

【0085】

また、L2SW10aのポートには、それぞれのVLAN用にアドレスが割り振られていることは図13と同様である。このように、VLAN-IDが付与されていない複数のイーサネットフレームを受信した場合でも、該当するVLANのEoEヘッダHを効率よく 50

設定することができる。

【0086】

次にEoEヘッダHのアドレス構成について説明する。図15はEoEヘッダHのアドレス構成例を示す図である。EoEヘッダHのSA、DA共に、48ビットのアドレス構成である。

【0087】

EoEヘッダHのSAは、送信元スイッチID、加入者インタフェースID、入力ポートIDから構成される（それぞれのフィールドのビット数は48ビット内で任意）。EoEヘッダHのDAは、宛先スイッチID、加入者インタフェースID、出力ポートIDから構成される（それぞれのフィールドのビット数は48ビット内で任意）。なお、スイッチIDとは、L2SW10のIDのことであり、加入者インタフェースIDとは、加入者インタフェース部101-1～101-nのIDのことである。 10

【0088】

このように、階層化イーサネット網2内で、EoEヘッダHに対して、物理トポロジのアドレスを独自に設けることにより（ネットワーク側のキャリアが使いやすいようにアドレスを設定する）、VPNを設定する際に、階層化イーサネット網2上で最短のパスでフレームを流すことが可能になる。

【0089】

図16はEoEヘッダHのアドレス構成例を示す図である。アドレス構成として他の例を示すものである。EoEヘッダHのSA、DA共に、48ビットのアドレス構成である。 20

【0090】

EoEヘッダHのSAは、VLAN-ID（すなわちVPN-ID）、送信元ユーザサイトIDから構成される（それぞれのフィールドのビット数は48ビット内で任意）。EoEヘッダHのDAは、VLAN-ID（すなわちVPN-ID）、宛先ユーザサイトIDから構成される（それぞれのフィールドのビット数は48ビット内で任意）。このようなアドレス構成にした場合には、テーブルサイズを小さくすることができるので、簡易な運用制御が可能になる。

【0091】

次にプライオリティ情報（図18で上述したTCI中のPriorityのこと）を有するEoEヘッダについて説明する。図17は階層化イーサネットフレームの構成を示す図である。図に示す階層化イーサネットフレームF4は、プライオリティ情報を含むEoEヘッダH4を有している。図中の数字はオクテットを示す。 30

【0092】

L2SW10では、ヘッダ情報としては、EoEヘッダHのヘッダ情報しか読み取らないため、階層化イーサネット網2内のL2SW10間でプライオリティ情報にもとづく通信を行いたい場合には、EoEヘッダHにプライオリティ情報をマッピングしておく必要がある。

【0093】

ここで、VLANタグTag1が付与されたイーサネットフレームf4をカプセル化する場合、カプセル化処理部11は、VLANタグTag1をコピーする。そして、コピーしたVLANタグ内のVLAN-IDをall“0”に設定したVLANタグTag2を、EoEヘッダのSAとタイプの間に挿入する。このように生成されたEoEヘッダH4をイーサネットフレームf4に付与して、階層化イーサネットフレームF4を生成する。 40

【0094】

これにより、EoEヘッダH4のVLANタグTag2内にはプライオリティ情報が含まれているので、L2SW10間でプライオリティ情報にもとづく通信を行うことが可能になる。

【0095】

以上説明したように、本発明によれば、L2SW10で、EoEヘッダHを付与してカプセル化し、階層化イーサネットフレームFを生成することで、従来の4094を超えるV 50

LAN (VPN) を構成することが可能になる。また、本発明では、パス設定などのためのシグナリングプロトコルも不要となるため、簡易な運用が可能になる。

【0096】

(付記1) VPNの通信サービスを行う通信システムにおいて、ユーザMACフレームをユーザサイトから受信し、加入者インタフェースのアドレスであるエッジ送信元アドレス及び前記ユーザMACフレームを送信すべき出口エッジ側の加入者インタフェースのアドレスであるエッジ宛先アドレスを含み、任意のVPNを設定するための階層化ヘッダを付与して、前記ユーザMACフレームをカプセル化し、階層化MACフレームを生成するカプセル化処理部を有し、階層化ネットワークの入口エッジ側に配置される入口エッジ装置と、

10

前記階層化MACフレームを受信し、前記階層化ヘッダにより、前記エッジ宛先アドレスが自己の加入者インタフェースのアドレスであり、かつ同一VLAN内の入口エッジ装置から送信されてきたことを認識した場合に、前記階層化MACフレームから前記ユーザMACフレームを取り出してデカプセル化するデカプセル化処理部を有し、前記階層化ネットワークの出口エッジ側に配置される出口エッジ装置と、を有することを特徴とする通信システム。

【0097】

(付記2) 前記カプセル化処理部は、ユーザMACフレームからユーザヘッダを抽出してユーザ宛先アドレスを取得するユーザヘッダ抽出部と、ユーザ宛先アドレスとエッジ宛先アドレスとの対応テーブルであるカプセル化テーブルにもとづき、取得されたユーザ宛先アドレスをキーにして、エッジ宛先アドレスの検索を行うテーブル検索部と、検索成功時は、検索されたエッジ宛先アドレスと、エッジ送信元アドレスとを含む階層化ヘッダを生成する階層化ヘッダ生成部と、前記ユーザMACフレームに前記階層化ヘッダを付与する階層化ヘッダ付与部と、階層化MACフレーム用のFCSを計算するFCS計算部と、から構成されることを特徴とする付記1記載の通信システム。

20

【0098】

(付記3) テーブル検索失敗時、前記階層化ヘッダ生成部は、宛先アドレスリストの各アドレスと、エッジ送信元アドレスとを含む複数の階層化ヘッダの生成、またはマルチキャストアドレスと、エッジ送信元アドレスとを含む複数の階層化ヘッダの生成のいずれかの生成処理を行い、前記階層化ヘッダ付与部は、ユーザMACフレームをコピーして、複数の階層化ヘッダをそれぞれ付与することを特徴とする付記2記載の通信システム。

30

【0099】

(付記4) 前記デカプセル化処理部は、階層化ヘッダにより、エッジ宛先アドレスが自己の加入者インタフェースのアドレスであるか、かつ同一VLAN内の入口エッジ装置から送信されてきたフレームであるかを判断して有効性のチェックを行う有効性チェック部と、前記階層化ヘッダのエッジ送信元アドレスとユーザヘッダのユーザ送信元アドレスとの対応をカプセル化テーブルに学習するアドレス学習部と、階層化MACフレームから前記階層化ヘッダを分離してユーザMACフレームを生成する階層化ヘッダ分離部と、ユーザMACフレーム用のFCSを計算するFCS計算部と、から構成されることを特徴とする付記1記載の通信システム。

40

【0100】

(付記5) 前記入口エッジ装置は、それぞれ異なるVLANのユーザサイトから、VLANタグ付きのユーザMACフレームを、1つのポートで複数受信する場合、VLAN毎に割り当てたポートのアドレスと、VLAN毎に割り当てたカプセル化テーブルと、を設けてVLANに対応した階層化ヘッダを生成することを特徴とする付記1記載の通信システム。

【0101】

(付記6) 前記入口エッジ装置は、それぞれ異なるVLANのユーザサイトから、VLANタグを含まないユーザMACフレームを、1つのポートで複数受信する場合、送信元MACアドレスとVLANとの対応テーブルであるMACアドレステーブルと、VLAN

50

毎に割り当てたポートのアドレスと、VLAN毎に割り当てたカプセル化テーブルと、を設けてVLANに対応した階層化ヘッダを生成することを特徴とする付記1記載の通信システム。

【0102】

(付記7) 前記カプセル化処理部は、階層化ヘッダを物理トポロジを表すID、またはVPNを表すIDでアドレスを構成することを特徴とする付記1記載の通信システム。

【0103】

(付記8) 前記カプセル化処理部は、ユーザヘッダ内のVLANタグをコピーして、プライオリティ情報を階層化ヘッダ内に含ませることを特徴とする付記1記載の通信システム。

10

【0104】

(付記9) VPNの通信サービスを行う通信装置において、ユーザMACフレームをユーザサイトから受信し、加入者インタフェースのアドレスであるエッジ送信元アドレス及び前記ユーザMACフレームを送信すべき出口エッジ側の加入者インタフェースのアドレスであるエッジ宛先アドレスを含み、任意のVPNを設定するための階層化ヘッダを付与して、前記ユーザMACフレームをカプセル化し、階層化MACフレームを生成するカプセル化処理部と、前記階層化MACフレームを受信し、前記階層化ヘッダにより、前記エッジ宛先アドレスが自己の加入者インタフェースのアドレスであり、かつ同一VLAN内の入口エッジ装置から送信されてきたことを認識した場合に、前記階層化MACフレームから前記ユーザMACフレームを取り出してデカプセル化する 20
デカプセル化処理部と、を有する加入者インタフェース部と、階層化ネットワークのインタフェースを行う局側インタフェース部と、を有することを特徴とする通信装置。

【0105】

(付記10) VPNの通信サービスを行う通信方法において、ユーザMACフレームをユーザサイトから受信した際に、加入者インタフェースのアドレスであるエッジ送信元アドレス及び前記ユーザMACフレームを送信すべき出口エッジ側の加入者インタフェースのアドレスであるエッジ宛先アドレスを含み、任意のVPNを設定するための階層化ヘッダを付与することで、前記ユーザMACフレームをカプセル化して、階層化MACフレームを生成し、 30
前記階層化MACフレームを受信した際に、前記階層化ヘッダにより、前記エッジ宛先アドレスが自己の加入者インタフェースのアドレスであり、かつ同一VLAN内の入口エッジ装置から送信されてきたことを認識した場合に、前記階層化MACフレームから前記ユーザMACフレームを取り出してデカプセル化することを特徴とする通信方法。

30

【0106】

【発明の効果】

以上説明したように、本発明の通信システムは、入口エッジ装置では、任意のVPNを設定するための階層化ヘッダを付与して、ユーザMACフレームをカプセル化して、階層化MACフレームを生成し、出口エッジ装置で、階層化MACフレームからユーザMACフ 40
レームを取り出してデカプセル化する構成とした。これにより、イーサネットを利用したブリッジネットワーク上に、従来の設定数を超えてVPNを構成できるので、スケーラビリティ及び運用効率の向上を図ることが可能になる。

【図面の簡単な説明】

【図1】 本発明の通信システムの原理図である。

【図2】 イーサネット通信における本発明のカプセル化イメージを示す図である。

【図3】 L2SWの構成を示す図である。

【図4】 カプセル化処理部の構成を示す図である。

【図5】 カプセル化処理後の階層化イーサネットフレームを示す図である。

【図6】 デカプセル化処理部の構成を示す図である。

50

【図7】 階層化イーサネットフレームのマルチキャストを示す図である。

【図8】 イーサネットフレームとマルチキャスト時の階層化イーサネットフレームを示す図である。

【図9】 階層化イーサネットフレームの受信イメージを示す図である。

【図10】 転送されるイーサネットフレーム及び階層化イーサネットフレームを示す図である。

【図11】 フレーム応答を返信する様子を示す図である。

【図12】 転送されるイーサネットフレーム及び階層化イーサネットフレームを示す図である。

【図13】 L2 SWの1つのポートへ複数のイーサネットフレームが入力する場合の構成 10
を示す図である。

【図14】 L2 SWの1つのポートへ複数のイーサネットフレームが入力する場合の構成
を示す図である。

【図15】 EoEヘッダのアドレス構成例を示す図である。

【図16】 EoEヘッダのアドレス構成例を示す図である。

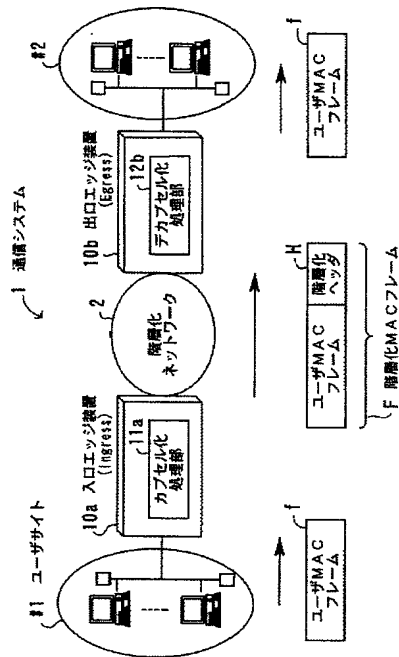
【図17】 階層化イーサネットフレームの構成を示す図である。

【図18】 VLAN使用時のフレームフォーマットを示す図である。

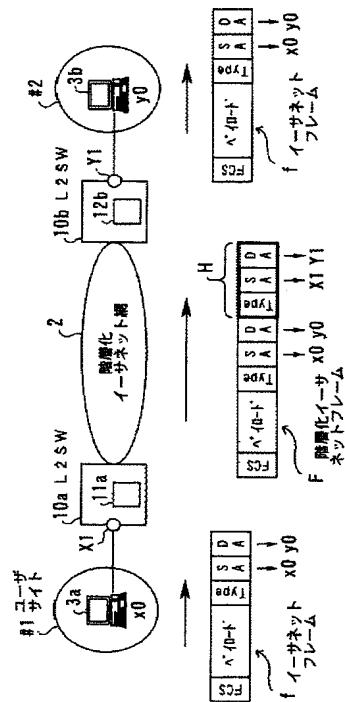
【符号の説明】

- 1 通信システム
- 2 階層化ネットワーク
- 10 a 入口エッジ装置
- 11 a カプセル化処理部
- 10 b 出口エッジ装置
- 12 b デカプセル化処理部
- #1、#2 ユーザサイト
- f ユーザMACフレーム
- F 階層化MACフレーム
- H 階層化ヘッダ

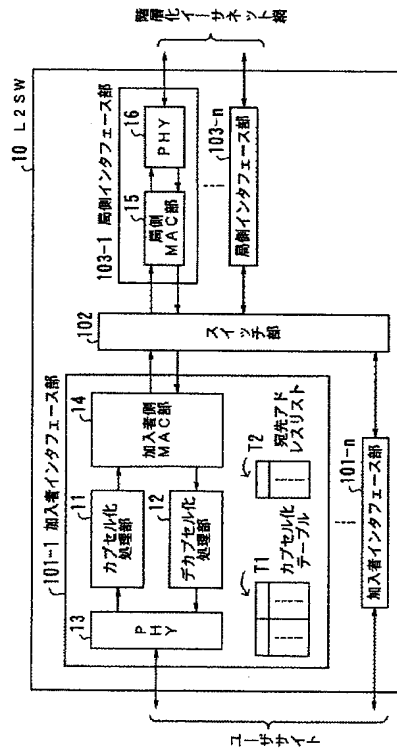
【図 1】



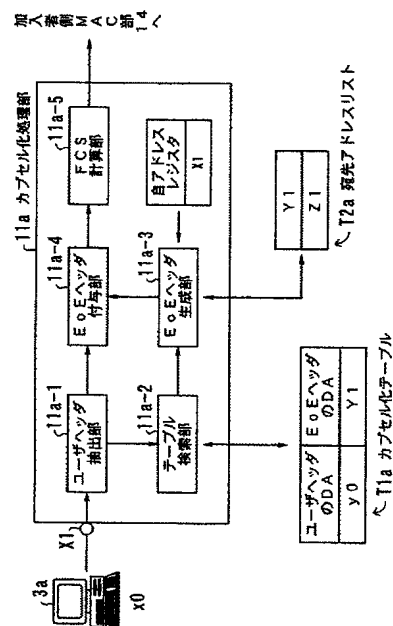
【図 2】



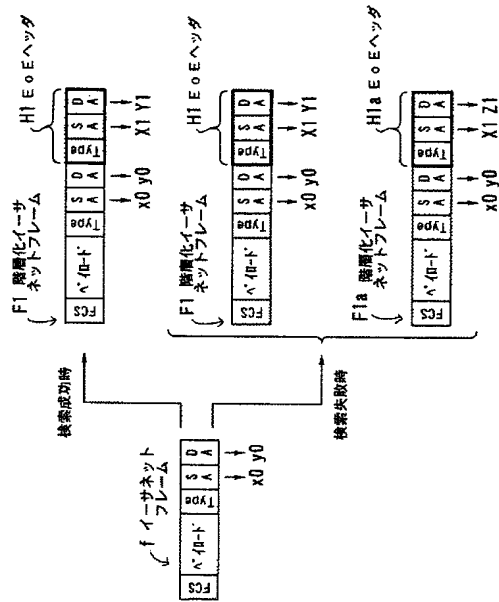
【図 3】



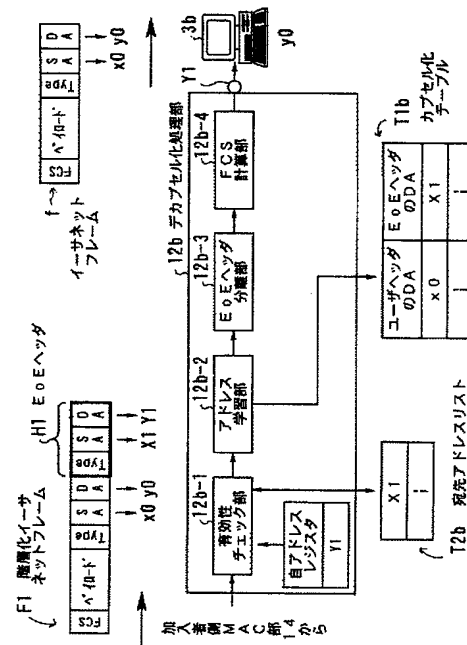
【図 4】



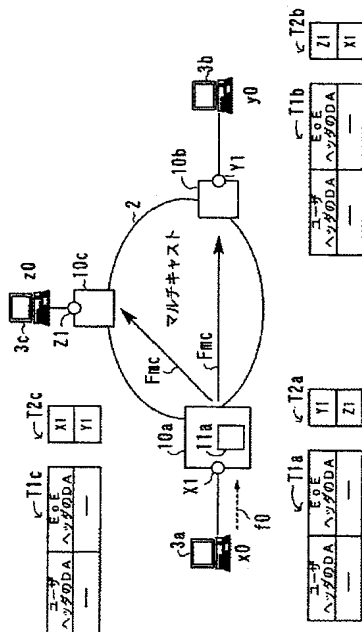
【図 5】



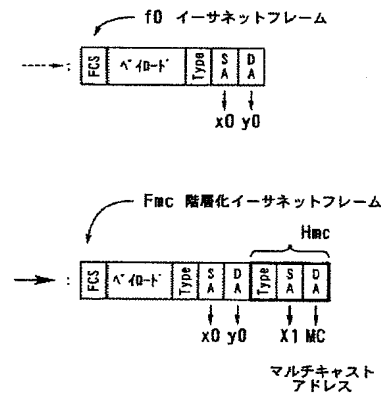
【図 6】



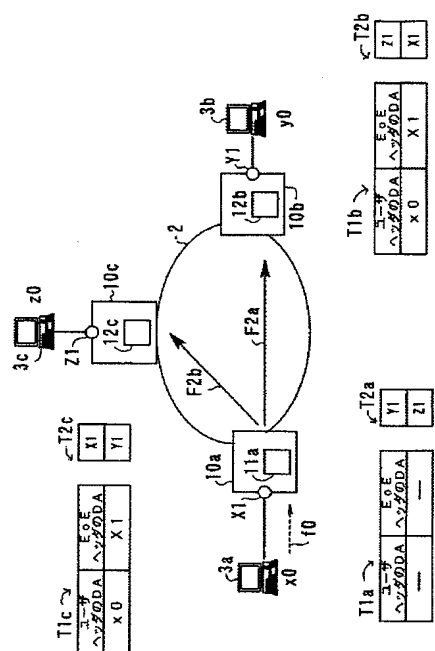
【図 7】



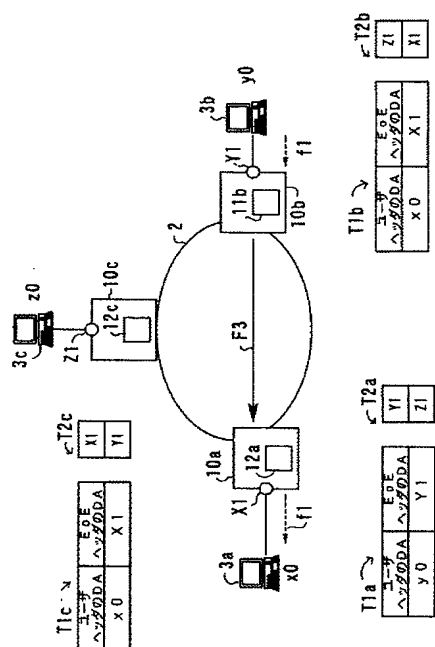
【図 8】



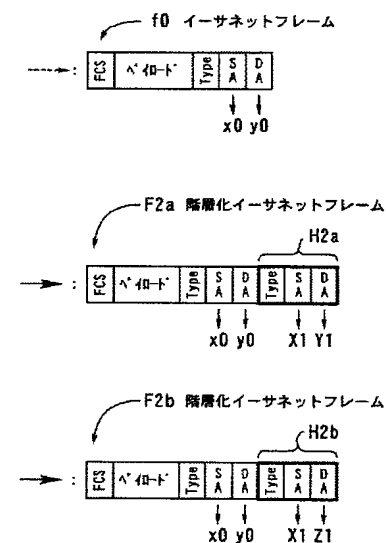
【図 9】



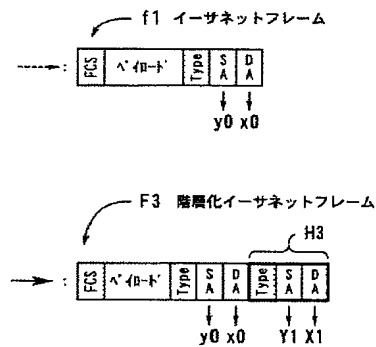
【図 1 1】



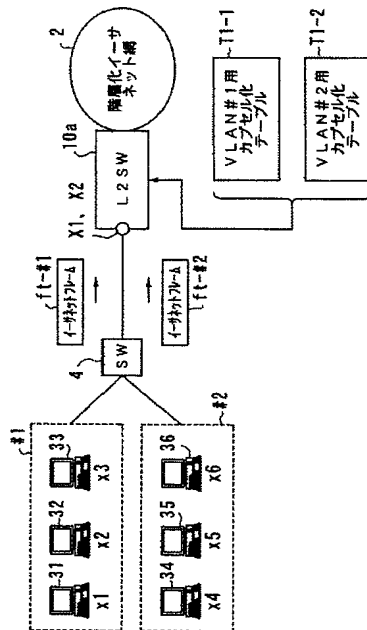
【図 1 0】



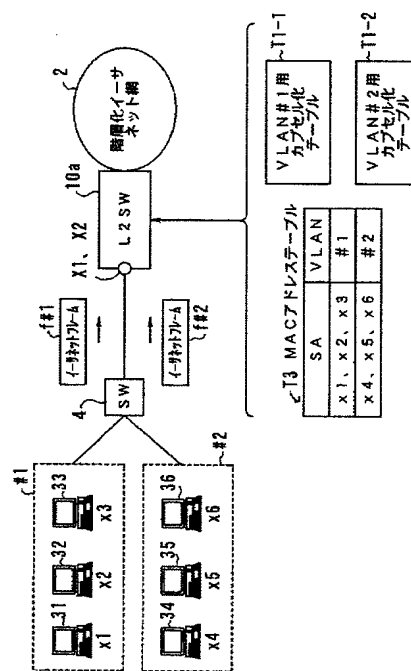
【図 1 2】



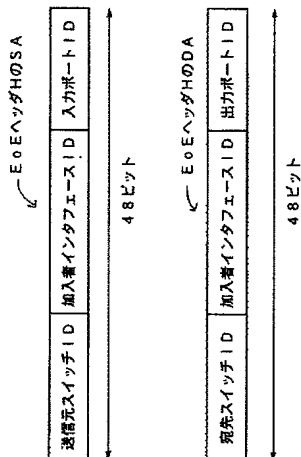
【図 13】



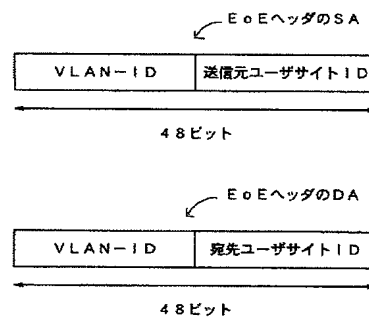
【図 14】



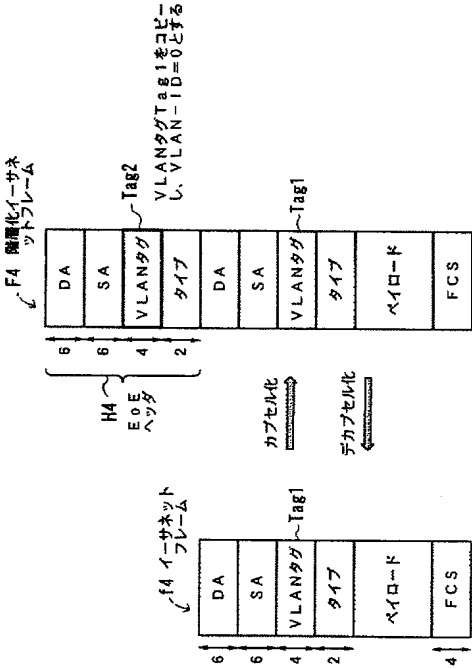
【図 15】



【図 16】



【図 17】



【図 18】

